1 Administration

Instructor: Leonard Schulman
Office: Jorgensen 288
Phone: (626) 395 6839
Office hours: W 10:30-12:00
Email: schulman@cs.caltech.edu
Secretary: Diane Goodfellow, Jorgensen 266, x6842, diane@cs
Course Web page: http://www.cs.caltech.edu/∼cs138/index.html

Teaching Assistants: Josh Bao (baodog@its.caltech.edu), Miroslav Dudik (miro@caltech.edu), Elitza Maneva (elitza@its.caltech.edu), Eugene Zarakhovsky (eugenez@its.caltech.edu).

TA office hours will be on [either Monday or Wednesday, TBA] and Thursday, from 7:00-8:30 in the VLSI lab (on the first floor of Jorgensen to the left of the entrance).

Problem sets will be posted on the web page on Fridays (usually already on Thursday evening), and due the following Friday by 4pm. You will be able to submit your work in one of two ways: (a) Electronically. Instructions will follow later. (b) Hardcopy. There will a box in the VLSI lab. Write each problem on a separate page, put your name on it, and submit in the proper folder that box. (N.B.: with this many sheets of paper there is always a slight danger we'll lose something. The TAs will be very careful, but I recommend you also keep a copy of your work.) Graded problem sets will be returned in the same box.

It is important that your work be written in clear technical English, and be typed or in legible handwriting. Points may reluctantly be deducted if these matters interfere with us reading your work.

Late policy: three times during the term you can submit your work three days late, by Monday at 4pm, without penalty. This will hopefully accomodate any conflicts, religious holidays, etc. If there is a very exceptional circumstance (e.g. an extended illness), please see me. Outside of these three occasions, work handed in by the "late deadline" will be penalized 25%. Work handed in past the "late deadline" will receive no credit. When you hand in late work, you must clearly indicate at the top of the assignment that it is being handed in late. If this is not a "free late", then you will be charged the 25% penalty only on the problems handed in late. You can choose to save your "free lates"; this can be advantageous if, for example, you just want to submit one or two problems late on an assignment early in the term. So, when handing in late work, you should indicate "late with penalty" or "free late". If you don't indicate which, you'll be charged a "free late". It is your responsibility to keep track of how many free lates you've used up.

You are permitted to collaborate with other students on the assignments but you should read and think about each problem alone for at least a few minutes; its wise to restrict your collaborations to the harder problems, and not to become dependent on this process. In any case, your submission must be written entirely on your own after the collaboration session is over – without reference to any notes made while collaborating. Also, as a matter of intellectual courtesy, indicate who you worked with on a problem. (This need not be reciprocal. If A was stuck on a problem until getting an idea from B who had already solved it, then no annotation is needed on B's assignment.)

There are two required books: Kozen, "The Design and Analysis of Algorithms", Springer-Verlag 1992, and Vasek Chvatal, "Linear Programming", W. H. Freeman, 1983. There are two recommended books: Cormen, Leiserson and Rivest, "Introduction to Algorithms", MIT Press 1990, and Stinson, "Cryptography: theory and practice", CRC Press, 1995.

You are welcome to take advantage of other sources. However, realize that some of the problems I'll assign are "standards", and solutions to those might be found in textbooks, notebooks of older students, and so forth. Regardless of the source, don't read existing solutions before turning in your work.

I encourage you to take advantage of office hours. We'll keep the web page up to date if those hours change. I generally won't discuss material over email.

There will be a final but no midterm. Your grade will be based 70% on the homeworks and 30% on the final.

If you aren't on the class mailing list, email Miro.

2 Problem Set # 10

1. **(5 points)** Describe a monotone non-increasing function $\nu : \mathbb{N} \to \mathbb{R}_{\geq 0}$ that is neither negligible nor nonnegligible.

2. **(5 points)** Here is an alternate definition of strong one way functions; call this class of functions, SOF′, and the class defined in lecture, SOF.

   Definition 1 *A function $f : \{0,1\}^* \to \{0,1\}^*$ is in SOF′ if:*

   (a) There exists a PPT F such that $F(x) = f(x)$.

   (b) There exist positive constants c_1, c_2 such that $|x|^{c_1} \leq |f(x)| \leq |x|^{c_2}$.

   (c) For every PPT A there is a negligible function ν such that

   $$P(f(A(f(x))) = f(x) : x \in_U \{0,1\}^k) \leq \nu(k).$$

   Show that SOF′ $\subseteq$ SOF. Then show how to modify any $f \in$ SOF so that it becomes a function in SOF′.

3. **(10 points)** Show how to construct a length-preserving strong one way function g, given a strong one way function f. (You can assume that f is in either SOF or SOF′ for the purpose of this exercise; just state which assumption you're using.)

4. **(10 points)** Recall the definition of **BPP** (notes for lecture 24).

   (a) Let $L \subseteq \{0,1\}^*$ and $b > 0$. Suppose that there is a PPT A such that for $x \in L$, $P(A(x) = 1) \geq \frac{1+|x|^{-b}}{3}$, and for $x \notin L$, $P(A(x) = 1) \leq \frac{1-|x|^{-b}}{3}$.

   Show that there is a PPT A such that for $x \in L$, $P(A(x) = 1) \geq \frac{1+|x|^{-b}}{2}$, and for $x \notin L$, $P(A(x) = 1) \leq \frac{1-|x|^{-b}}{2}$.

   (b) Suppose that there is a PPT A such that for $x \in L$, $P(A(x) = 1) \geq \frac{1+|x|^{-b}}{2}$, and for $x \notin L$, $P(A(x) = 1) \leq \frac{1-|x|^{-b}}{2}$. Show that $L \in$ **BPP** .

   (c) Show that if $L \in$ **BPP** then there is a PPT for L which errs with probability at most e^{-n} on inputs of length n.

   Hint: for this exercise you need to use the large deviation bound known as the Chernoff bound. You can find it in a probability textbook.

5. **(10 points)** In this exercise we'll consider a "permutation" $\pi : \{0,1\}^* \to \{0,1\}^*$ to be a function which is length preserving and acts as a permutation on each set $\{0,1\}^n$. A strong one way permutation (SOP) is a strong one way function which is also a permutation. A PPT permutation is one which can be computed by a PPT. The composition $h = g \circ f$ of two functions is the function $h(x) = g(f(x))$.

   (a) Show that if f is a SOP and π is a PPT then $\pi \circ f$ is a SOP.

   (b) Assume that there exist strong one way functions. Show that there is a SOF f_1 and another SOF f_2 such that $f_2 \circ f_1$ is not a SOF.

6. **(**10 **points)** The definition we saw for the notion of "poly-time indistinguishable" (sequences of) distributions Q and R, suggests that we also use the following definition:

Definition 2 *Q and R are "poly-time distinguishable" if there exists a PPT test T such that*

$$|P_{x \leftarrow Q_n}(T(x) = 1) - P_{x \leftarrow R_n}(T(x) = 1)|$$

is a nonnegligible function. (Observe, this is a little stronger than demanding that Q and R fail test T.)

However, there is something worrisome about this definition. What use is it that $|P_{x \leftarrow Q_n}(T(x) = 1) - P_{x \leftarrow R_n}(T(x) = 1)|$ is "large", if you don't know which of $P_{x \leftarrow Q_n}(T(x) = 1)$ or $P_{x \leftarrow R_n}(T(x) = 1)$ is greater?

Prove that if Q and R are poly-time distinguishable (by the above definition), then there exists a PPT T' for which

$$P_{x \leftarrow Q_n}(T'(x) = 1) - P_{x \leftarrow R_n}(T'(x) = 1)$$

is positive and nonnegligible.